

From: [redacted]
Sent: Tuesday, January 16, 2007 9:51 AM
To: Taskforcecomments
Subject: Comments

There is currently nothing in place to prevent someone from opening a checking account in another person's name. The banks do not run a credit reports, because if they did they would see many of these people were already victims of identity theft and there are hawk alerts in place. They do not verify the address, which often times does not even match up with the counterfeit identification presented at the time the account is opened. They are not alerted when they have multiple accounts set up at the same fraud address and they do not even catch on when the victim already has an existing account at another address. The only time they do SARs is when they suffer a loss and when law enforcement is attempting to conduct an investigation they provide copies of documents relating to their losses and fail to mention there were checks returned to other financial institutions. When a Bank Investigator presents a case to law enforcement, they should know what is needed for prosecution, including any original documents and suspect photos.

The Task Force should request that all financial institutions require their customers to take a photo upon opening a new account. This will be part of the customer's signature card, which ideally would bear a thumb print. When a customer comes to make a deposit, or cash a check, the teller would see the photo on file and at least see if this is indeed their account holder. If it is later learned this is a fraudulent account, law enforcement has a good photo of the individual. This same photo could be provided to Secretary of State Police to conduct a facial recognition search to see what other names the suspect may be using. At some point the banks themselves may have this same capability to see if the suspect has multiple accounts with them and to share the photo with other financial institutions. There are already lap top computers, which can only be turned on with the owner's finger print - this same technology can be used at teller windows and ATMs in place of pin numbers. It would pretty hard for a suspect to deny he was the one involved in a transaction activated by his or her fingerprint. The banks may claim this would be too costly, but if one major financial institution would take the lead on this and promote themselves as the bank that was truly concerned with identity theft - the other banks would jump on board. However, it would be easier if government regulations required them all to have the same security measures.

I'm always amazed how many people comment on the photo I have on my credit card. How difficult would it be to require every credit card to contain the cardholder's photo? At least when we arrest a suspect with

credit cards he had fraudulently applied for, he can't deny someone else had applied for them. The same mag strips, which already contain so much information on a credit card, can easily hold a digital image of the cardholder. If these financial institutions were willing to spend the same kind of money on their security features, as they do on their advertising, I'm sure they could create credit card terminals which would display the cardholder's photo to the clerk at the Point Of Sale. Instead of seeing if the signature on the card matched the signature on the customer's receipt, the clerk would be looking at the image on the terminal screen and comparing that to the customer standing there. Ideally, this same image could later be retrieved for investigative purposes. Credit cards should not be activated from a telephone call, but the customer should be required to enter a financial institution and once again a fingerprint is provided. If the account is discovered to be associated to identity theft the bank now has a print and photo to supply law enforcement and this print can obviously be run through AFIS to see if the suspect has been arrested before.

There has been so much media attention to identity theft recently that I'm sure most consumers would not see these request by the banks as being intrusive and they would be very receptive to having these security measures implemented.